UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
4523 N. 24th Place, Milwaukee, Wisconsin, more fully described in Attachment A.

Case No. 25-949M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 6/12/2025 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph, U.S. Magistrate .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: 5/30/2025 3:13 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

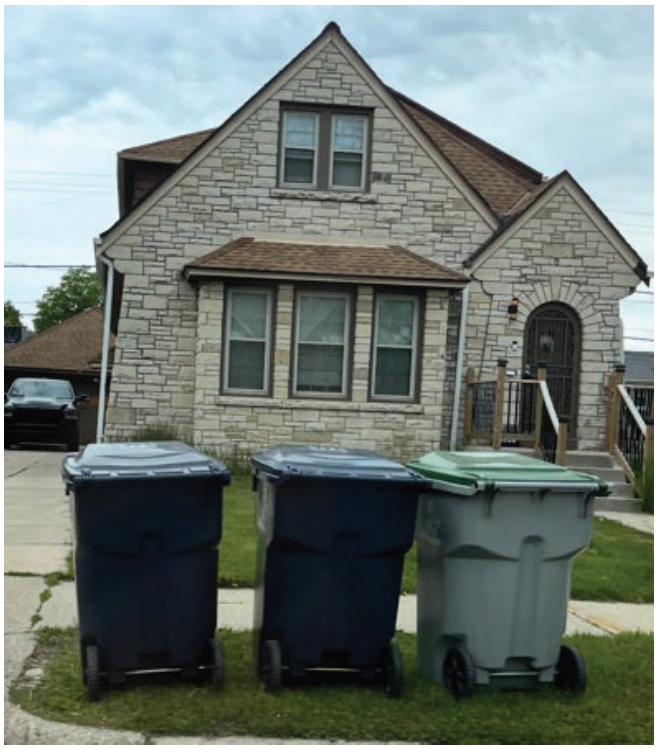
_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

PLACE TO BE SEARCHED

4523 N. 24th Place, Milwaukee, Wisconsin (TARGET LOCATION) – to include its occupants. This is the residence of Jesus PUENTES. The residence is described as a two story duplex residence. The residence has a tan brick front with a brown shingled roof. The front door has a black or dark colored iron security storm door and there is a wooden and metal railed porch around the front door area that sits on top of concrete steps. There are no visible numbers on the front of the residence, but there is a ring style security doorbell camera affixed to the left side of the door. There is also an entry door visible on the south side of the residence accessible from the driveway. The numbers 4523A are visible above the entry door that is on the south side of the residence. The residence has a detached garage with a brown garage door and brown shingled roof that sits behind the residence.



ATTACHMENT B

ITEMS TO BE SEIZED

All records, information, and items relating to violations of 18 USC §922(g)(1), 21 U.S.C. §§ 841(a)(1), 843 and 846, including:

a. Evidence of the crimes described above;

b. Preparatory steps taken in furtherance of those crimes;

c. Evidence of the existence, scope, or overt acts in furtherance of a conspiracy;

d. Evidence of motive, intent, or knowledge of the crime described above;

e. Evidence of the location, whereabouts, and patterns of travel of Jesus PUENTES;

f. Evidence about the appearance, clothing, and identity of Jesus PUENTES;

g. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances and counting drug proceeds;

h. Containers to hold or transport controlled substances and drug trafficking related items and proceeds;

i. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;

j. Firearms, including pistols, handguns, shotguns, rifles, assault weapons, machine guns, magazines used to hold ammunition, silencers, components of firearms including laser sights and other components which can be used to modify firearms, ammunition and ammunition components, bulletproof vests, gun boxes and any and all documentation related to the purchase of such items;

k. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;

l. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents

noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

m. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

n. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

o. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;

p. Indicia of occupancy, residency or ownership of the premises, vehicles, and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

q. Photographs, videotapes or other depictions of assets, coconspirators, controlled substances, or other paraphernalia associated with drug trafficking;

r. Evidence indicating how and when electronic devices were accessed or used, to determine the chronological and geographic context of access, use, and events relating to the crime under investigation; and

s. Cellular telephones, text messaging systems, other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;

t. Computers, laptops, or other electronic storage device capable of being used to commit the violations or store any of the information described above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

During the execution of the search of the locations or person described in Attachments A, law enforcement personnel are authorized (1) to press the fingers (including thumbs) of any individuals found at the **TARGET LOCATION** to the fingerprint sensor ("Touch ID") and (2) to present the face of any individuals found at the **TARGET LOCATION** to the facial recognition sensor, such as a camera, ("Face ID") of the device found at the **TARGET LOCATION** for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Note: The government will attempt to retrieve and copy all data from computers found at the location to be searched without physically removing said computers. If occupants of the premises are unwilling to cooperate with the agent(s) regarding the operation of an on-site computer system(s), and/or it appears that there is/are data security devices involved, or the computer system utilizes unusual or proprietary equipment, the computer system may be seized, along with the proprietary equipment. If the agent determines that the volume of material found on the premises is voluminous in size, and/or for any technical reason the agent(s) on the scene cannot search for or image/copy the information found on the premises, the computer system(s) and media may be seized.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

4523 N. 24th Place, Milwaukee, Wisconsin, more fully described in Attachment A.

Case No. 25-949M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. 841 & 846	Possession with the intent to distribute a controlled substance; Conspiracy to possess with the intent to distribute controlled substances; felon in possession of a firearm.
18 U.S.C. 922(g)(1)	

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

TYLER OWENBY Digitally signed by TYLER OWENBY Date: 2025.05.30 14:13:06 -05'00'

Applicant's signature

Tyler F. Owenby, DEA Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 05/30/2025

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Tyler F. Owenby, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Drug Enforcement Administration ("DEA"). I have been so employed since July 2021 and am currently assigned to the DEA Milwaukee District Office. As part of my duties as a DEA Special Agent, I investigate criminal violations relating to narcotics trafficking and money laundering offenses, including criminal violations of the Federal Controlled Substance laws, including, but not limited to Title 18, United States Code, Sections 1956, and 1957, and Title 21, United States Code, Sections 841, 843, 846, 848, 952 and 963. I have been involved in electronic surveillance methods, the debriefing of defendants, informants, and witnesses, as well as others who have knowledge of the distribution, transportation, storage, and importation of controlled substances.

2. Prior to my employment with the DEA, I spent the previous five years working as an Analyst assigned to the Columbia Missouri Police Department's Vice Narcotics and Organized Crime Unit. As part of my duties as an Analyst, I was formally trained and certified in the areas of mobile phone forensics, cell tower and phone toll analysis, and advanced open source intelligence gathering techniques.

3. I have participated in complex narcotics investigations which involved violations of state and federal controlled substances laws and money laundering laws including Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, and Title 18, United States Code, Sections 1956 and 1957, and other related offenses. More specifically, my training and experience includes the following:

a. I have utilized informants to investigate drug trafficking. Through informant interviews, and extensive debriefings of individuals involved in drug trafficking, I have learned about the manner in which individuals and organizations distribute controlled substances in Wisconsin and throughout the United States;

b. I have experience conducting street surveillance of individuals engaged in drug trafficking. I have participated in the execution of search warrants where controlled substances, drug paraphernalia, and drug trafficking records were seized;

c. I am familiar with the appearance and street names of various drugs, including marijuana, heroin, cocaine, cocaine base (unless otherwise noted, all references to crack cocaine in this affidavit is cocaine base in the form of crack cocaine), ecstasy, and methamphetamine. I am familiar with the methods used by drug dealers to package and prepare controlled substances for sale. I know the street values of different quantities of the various controlled substances;

d. I know that drug traffickers often use electronic equipment and wireless and land line telephones to conduct drug trafficking operations. I am familiar with the language utilized over the telephone or other communication applications to discuss drug trafficking, and know that the language is often limited, guarded, and coded. Additionally, I know that drug traffickers often change their phone numbers and cellular devices on frequent basis in an attempt to thwart law enforcement from tracking their phones and to conceal their identity.

e. I know that drug traffickers commonly have in their possession, and at their residences and other locations ("stash houses") where they exercise dominion and control, controlled substances, firearms, ammunition, drug proceeds, and records or receipts pertaining their drug trafficking;

f. I know that drug traffickers used what is refer to as a "stash house" to stow illegal items such as illegal controlled substance, packaging paraphernalia, illegal firearms, ledgers, and US currency. Often times members of drug trafficking organizations have to make stops at the stash locations to pick up illegal controlled substance to deliver. Additionally, drug traffickers will have customers meet drug traffickers near the stash location. Multiple stops can be made in a day at these locations. This is done so the trafficker does not have to carry additional illegal controlled substances in their vehicle or person or maintain them at their residence. This protects the trafficker from law enforcement investigations as they do not have illegal controlled substances on them after the delivery is made or inside their personal residence. Often time the US currency will be transported after the delivery to the stash house to protect against law enforcement investigation and rival drug trafficker's robbery crews.

g. I know that drug traffickers often put their telephones in nominee names in order to distance themselves from telephones that are utilized to facilitate drug trafficking; and

h. I know that drug traffickers often use drug proceeds to purchase assets such as vehicles, property, and jewelry. I also know that drug traffickers often use nominees to purchase and/or title these assets in order to avoid scrutiny from law enforcement officials.

4. I have participated in numerous investigations involving the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these devices. I have also participated in investigations involving the use of historical and prospective location information to identify targets, map patterns of travel, corroborate other evidence, and apprehend persons to be arrested. On numerous occasions, this electronic evidence has provided proof of the crimes being investigated and corroborated information already known or suspected by law enforcement. During the course of my investigations, I have regularly used electronic evidence relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of co-conspirators.

5. The facts in this affidavit come my personal participation in this investigation, and my review of other federal, state, and local law enforcement agents and officers, all of whom I believe to be truthful and reliable. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation.

7. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 922(g)(1) (felon in possession of a firearm), Title 21, United States Code, Sections 841(a)(1), 846 (possession with intent to distribute and conspiracy to possess with the intent to distribute a controlled substance) have been committed, are being committed, and will be committed by Jesus PUENTES (DOB:XX/XX/1986) and others known and unknown to case agents. There is also probable cause to search the location described in Attachment A for evidence of these crimes, as described in Attachment B.

PLACE TO BE SEARCHED

8. This affidavit is submitted in support of applications for search warrants to seek evidence of violations of Title 18, United States Code, Sections 922(g)(1) (felon in possession of a firearm), Title 21, United States Code, Sections 841(a)(1), 846 (possession with intent to distribute and conspiracy to possess with the intent to distribute a controlled substance); for the following location (**"TARGET LOCATION")** associated with Jesus PUENTES, who has committed, are committing, and will continue to commit the above-listed offenses:

a. 4523 N. 24th Place, Milwaukee, Wisconsin, is a two story duplex residence. The residence has a tan brick front with a brown shingled roof. The front door has a black or dark colored iron security storm door and there is a wooden and metal railed porch around the front door area that sits on top of concrete steps. There are no visible numbers on the front of the residence, but there is a ring style security doorbell camera affixed to the left side of the door. There is also an entry door visible on the south side of the residence accessible from the driveway. The numbers 4523A are visible above the entry door that is on the south side of the residence. The residence has a detached garage with a brown garage door and brown shingled roof that sits behind the residence.

PROBABLE CAUSE

9. On May 30, 2025, the United States Marshals Service Great Lakes Regional Fugitive Task Force (GLRFTF) responded to 4523 N. 24th Place, Milwaukee, Wisconsin, to take

Jesus PUENTES into custody regarding outstanding state of Wisconsin felony warrants. Members of the GLRFTF responded to the residence and began knocking and announcing. After knocking and announcing PUENTES came to the door on the south side of the residence near the driveway and was taken into custody without incident. While members of the GLRFTF were searching PUENTES incident to his arrest small amounts of suspected cocaine were located in PUENTES front right pants pocket. PUENTES stated to arresting officers, "it's just my snorting powder."

10. While clearing the **Target Residence** for additional occupants, GLRFTF personnel noted a semi-automatic Glock handgun in the front east bedroom area of the upper portion of the duplex in plain view. Agents located a black bag in the northeast bedroom. The bag was open and agents observed in plain view a plastic baggie containing blue pills that appeared to be bagged for distribution.

11. PUENTES was convicted in 2004 of possession with intent cocaine and subsequently is a convicted felon who is prohibited from possession firearms.

12. Members of DEA Milwaukee responded to the scene and are currently holding the **Target Residence** for the application of a federal search warrant. PUENTES was already known to Milwaukee DEA through previous investigation as a kilogram level fentanyl and cocaine dealer operating in the city of Milwaukee.

TECHINCAL BACKGROUND

13. I know based upon my training and experience that controlled substances and evidence of narcotics trafficking can be secreted in any part of a residence including garages, storage areas related to the premises, vehicles on and associated with the premises, and on persons engaged in drug trafficking within the residence. I know through personal training and experience in investigating drug trafficking, controlled substances are frequently stored with drug proceeds,

other drug paraphernalia and documentation of drug trafficking at drug traffickers' residences and stash houses; that the execution of a search warrant usually results in the seizure of such items of personal property as utility bills, canceled mail envelopes, bank statements, keys, photographs, videotapes, and other items or documents which establish the identities of persons residing in or having control of the premise; and that these items can be stored in various locations accessible to the target location including vehicles and garages. Therefore, I believe it is reasonable to believe that an individual engaged in drug trafficking would conceal evidence related to drug trafficking in multiple areas associated with their residence including vehicles, garages and basements and on their person.

14. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **TARGET LOCATION**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, cellular telephone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

15. *Probable cause.* I submit that if a computer, cellular telephone, or storage medium is found on the **TARGET LOCATION**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET LOCATION** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media,

and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy

evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

17. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often

requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying

storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC UNLOCK

19. The warrant I am applying for would permit law enforcement to obtain from the display of physical biometric characteristics (such as fingerprint, thumbprint, facial, or iris characteristics) to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

20. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices, and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to use.

21. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home"

button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

22. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device through his or her irises. For example, Samsung offers an Iris Scanner, which uses the biometric information of an individuals' irises to identify the user.

23. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

24. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the

device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

25. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered within a certain period of time. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

26. Due to the foregoing, with respect to any person who is located in the **TARGET LOCATION** during the execution of the search and who is reasonably believe by law enforcement to be a user of a biometric sensor-enabled device that falls within the scope of this warrant, it is requested that law enforcement personnel may (1) press or swipe the fingers (including thumbs) of the person to the fingerprint scanner of the device found at the premises; or (2) hold the device in front of the person's face to activate the facial and/or iris recognition features, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

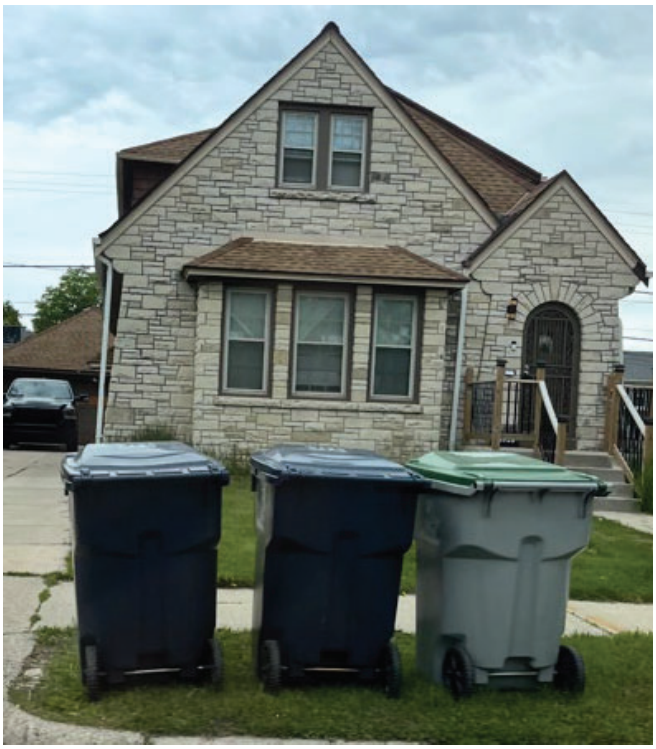
27. Based on the foregoing, I believe there is probable cause to believe Jesus PUENTES (DOB:XX/XX/1986) has committed violations of Title 18, United States Code, Sections 922(g)(1) (felon in possession of a firearm), Title 21, United States Code, Sections

841(a)(1), 846 (possession with intent to distribute and conspiracy to possess with the intent to distribute a controlled substance). I further believe that there is probable to believe that located at and in the **TARGET LOCATION** further described in attachment A, there is evidence of these crimes, all of which is detailed more specifically in Attachment B, that a warrant issued authorizing the search of the same. I further believe that there is probable cause to believe that located at and in the **TARGET LOCATION** described in Attachment A, there is evidence of the Target Offenses. Case agents believe there are currently documents and records showing dominion and control of the **TARGET LOCATION** and subject vehicle, cellular telephones, electronic devices, and other computers, and other evidence evincing the PUENTES' involvement in the drug trafficking offenses described above, located within the premise, vehicle, and person described in Attachments A. For all of the foregoing reasons, I request authorization to search the premise, vehicle, and person more fully described in Attachments A for the things described in Attachment B.

ATTACHMENT A

PLACE TO BE SEARCHED

4523 N. 24th Place, Milwaukee, Wisconsin (TARGET LOCATION) – to include its occupants. This is the residence of Jesus PUENTES. The residence is described as a two story duplex residence. The residence has a tan brick front with a brown shingled roof. The front door has a black or dark colored iron security storm door and there is a wooden and metal railed porch around the front door area that sits on top of concrete steps. There are no visible numbers on the front of the residence, but there is a ring style security doorbell camera affixed to the left side of the door. There is also an entry door visible on the south side of the residence accessible from the driveway. The numbers 4523A are visible above the entry door that is on the south side of the residence. The residence has a detached garage with a brown garage door and brown shingled roof that sits behind the residence.



ATTACHMENT B

ITEMS TO BE SEIZED

All records, information, and items relating to violations of 18 USC §922(g)(1), 21 U.S.C. §§ 841(a)(1), 843 and 846, including:

a. Evidence of the crimes described above;

b. Preparatory steps taken in furtherance of those crimes;

c. Evidence of the existence, scope, or overt acts in furtherance of a conspiracy;

d. Evidence of motive, intent, or knowledge of the crime described above;

e. Evidence of the location, whereabouts, and patterns of travel of Jesus PUENTES;

f. Evidence about the appearance, clothing, and identity of Jesus PUENTES;

g. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances and counting drug proceeds;

h. Containers to hold or transport controlled substances and drug trafficking related items and proceeds;

i. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;

j. Firearms, including pistols, handguns, shotguns, rifles, assault weapons, machine guns, magazines used to hold ammunition, silencers, components of firearms including laser sights and other components which can be used to modify firearms, ammunition and ammunition components, bulletproof vests, gun boxes and any and all documentation related to the purchase of such items;

k. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;

l. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents

noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

m. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

n. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

o. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;

p. Indicia of occupancy, residency or ownership of the premises, vehicles, and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

q. Photographs, videotapes or other depictions of assets, coconspirators, controlled substances, or other paraphernalia associated with drug trafficking;

r. Evidence indicating how and when electronic devices were accessed or used, to determine the chronological and geographic context of access, use, and events relating to the crime under investigation; and

s. Cellular telephones, text messaging systems, other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;

t. Computers, laptops, or other electronic storage device capable of being used to commit the violations or store any of the information described above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

During the execution of the search of the locations or person described in Attachments A, law enforcement personnel are authorized (1) to press the fingers (including thumbs) of any individuals found at the **TARGET LOCATION** to the fingerprint sensor ("Touch ID") and (2) to present the face of any individuals found at the **TARGET LOCATION** to the facial recognition sensor, such as a camera, ("Face ID") of the device found at the **TARGET LOCATION** for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Note: The government will attempt to retrieve and copy all data from computers found at the location to be searched without physically removing said computers. If occupants of the premises are unwilling to cooperate with the agent(s) regarding the operation of an on-site computer system(s), and/or it appears that there is/are data security devices involved, or the computer system utilizes unusual or proprietary equipment, the computer system may be seized, along with the proprietary equipment. If the agent determines that the volume of material found on the premises is voluminous in size, and/or for any technical reason the agent(s) on the scene cannot search for or image/copy the information found on the premises, the computer system(s) and media may be seized.